## **Step 1: Create a Gateway Load Balancer**

Use the following procedure to create your load balancer, listener, and target group.

###### **To create the load balancer, listener, and target group using the console**

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the navigation pane, under Load Balancing, choose Load Balancers.
3. Choose Create load balancer.
4. Under Gateway Load Balancer, choose Create.
5. Basic configuration
   1. For Load balancer name, enter a name for your load balancer.
   2. For IP address type, choose IPv4 to support IPv4 addresses only or Dualstack to support both IPv4 and IPv6 addresses.
6. Network mapping
   1. For VPC, select the service provider VPC.
   2. For Mappings, select all of the Availability Zones in which you launched security appliance instances, and one subnet per Availability Zone.
7. IP listener routing
   1. For Default action, select an existing target group to receive traffic. This target group must use the GENEVE protocol.  
      If you don't have a target group, choose Create target group, which opens a new tab in your browser. Choose a target type, enter a name for the target group, and keep the GENEVE protocol. Select the VPC with your security appliance instances. Modify the health check settings as needed, and add any tags that you need. Choose Next. You can register your security appliance instances with the target group now, or after you finish this procedure. Choose Create target group and then return to the previous browser tab.
   2. (Optional) Expand Listener tags and add the tags that you need.
8. (Optional) Expand Load balancer tags and add the tags that you need.
9. Choose Create load balancer.

## **Step 2: Create a Gateway Load Balancer endpoint service**

Use the following procedure to create an endpoint service using your Gateway Load Balancer.

###### **To create a Gateway Load Balancer endpoint service**

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose Endpoint services.
3. Choose Create endpoint service and do the following:
   1. For Load balancer type, choose Gateway.
   2. For Available load balancers, select your Gateway Load Balancer.
   3. For Require acceptance for endpoint, select Acceptance required to accept connection requests to your service manually. Otherwise, they are automatically accepted.
   4. For Supported IP address types, do one of the following:
      * Select IPv4 – Enable the endpoint service to accept IPv4 requests.
      * Select IPv6 – Enable the endpoint service to accept IPv6 requests.
      * Select IPv4 and IPv6 – Enable the endpoint service to accept both IPv4 and IPv6 requests.
   5. (Optional) To add a tag, choose Add new tag and enter the tag key and tag value.
   6. Choose Create. Note the service name; you'll need it when you create the endpoint.
4. Select the new endpoint service and choose Actions, Allow principals. Enter the ARNs of the service consumers that are allowed to create an endpoint to your service. A service consumer can be a user, IAM role, or AWS account. Choose Allow principals.

## **Step 3: Create a Gateway Load Balancer endpoint**

Use the following procedure to create a Gateway Load Balancer endpoint that connects to your Gateway Load Balancer endpoint service. Gateway Load Balancer endpoints are zonal. We recommend that you create one Gateway Load Balancer endpoint per zone. For more information, see [Access virtual appliances through AWS PrivateLink](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway-load-balancer.html) in the *AWS PrivateLink Guide*.

###### **To create a Gateway Load Balancer endpoint**

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose Endpoints.
3. Choose Create endpoint and do the following:
   1. For Service category, choose Other endpoint services.
   2. For Service name, enter the service name that you noted earlier, and then choose Verify service.
   3. For VPC, select the service consumer VPC.
   4. For Subnets, select a subnet for the Gateway Load Balancer endpoint.
   5. For IP address type, choose from the following options:
      * IPv4 – Assign IPv4 addresses to your endpoint network interfaces. This option is supported only if all selected subnets have IPv4 address ranges.
      * IPv6 – Assign IPv6 addresses to your endpoint network interfaces. This option is supported only if all selected subnets are IPv6 only subnets.
      * Dualstack – Assign both IPv4 and IPv6 addresses to your endpoint network interfaces. This option is supported only if all selected subnets have both IPv4 and IPv6 address ranges.
   6. (Optional) To add a tag, choose Add new tag and enter the tag key and tag value.
   7. Choose Create endpoint. The initial status is pending acceptance.

To accept the endpoint connection request, use the following procedure.

1. In the navigation pane, choose Endpoint services.
2. Select the endpoint service.
3. From the Endpoint connections tab, select the endpoint connection.
4. To accept the connection request, choose Actions, Accept endpoint connection request. When prompted for confirmation, enter **accept** and then choose Accept.

## **Step 4: Configure routing**

Configure the route tables for the service consumer VPC as follows. This allows the security appliances to perform security inspection on inbound traffic that's destined for the application servers.

###### **To configure routing**

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the navigation pane, choose Route tables.
3. Select the route table for the internet gateway and do the following:
   1. Choose Actions, Edit routes.
   2. Choose Add route. For Destination, enter the IPv4 CIDR block of the subnet for the application servers. For Target, select the VPC endpoint.
   3. If you support IPv6, choose Add route. For Destination, enter the IPv6 CIDR block of the subnet for the application servers. For Target, select the VPC endpoint.
   4. Choose Save changes.
4. Select the route table for the subnet with the application servers and do the following:
   1. Choose Actions, Edit routes.
   2. Choose Add route. For Destination, enter **0.0.0.0/0**. For Target, select the VPC endpoint.
   3. If you support IPv6, choose Add route. For Destination, enter **::/0**. For Target, select the VPC endpoint.
   4. Choose Save changes.
5. Select the route table for the subnet with the Gateway Load Balancer endpoint, and do the following:
   1. Choose Actions, Edit routes.
   2. Choose Add route. For Destination, enter **0.0.0.0/0**. For Target, select the internet gateway.
   3. If you support IPv6, choose Add route. For Destination, enter **::/0**. For Target, select the internet gateway.
   4. Choose Save changes.